

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-346211

(43) 公開日 平成11年(1999)12月14日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 L 9/38

H 0 4 L 9/00

6 9 1

H 0 4 B 10/00

H 0 4 B 9/00

Z

審査請求 未請求 請求項の数 4 O L (全 13 頁)

(21) 出願番号 特願平11-78858

(22) 出願日 平成11年(1999) 3 月24日

(31) 優先権主張番号 特願平10-83203

(32) 優先日 平10(1998) 3 月30日

(33) 優先権主張国 日本 (J P)

(71) 出願人 597139561

元吉 明夫

熊本県熊本市池田 3 丁目1272番地 2

(71) 出願人 597139572

松岡 正浩

熊本県熊本市黒髪 5 丁目 8 番26-502号

(72) 発明者 元吉 明夫

熊本県熊本市池田 3 丁目1272番地 2

(72) 発明者 松岡 正浩

熊本県熊本市黒髪 5 丁目 8 番26-502号

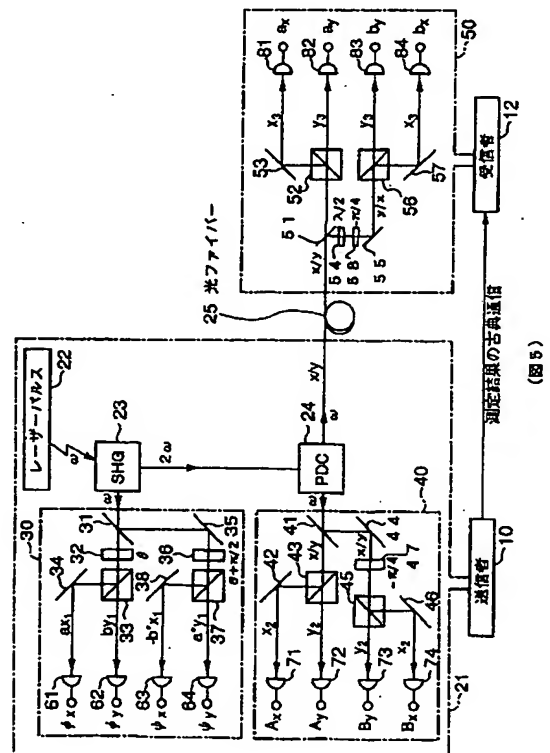
(74) 代理人 弁理士 加藤 卓

(54) 【発明の名称】 量子通信方法及び装置

(57) 【要約】

【課題】 量子ビットのテレポーテーションの考え方を実現できる量子通信方法及び装置を提供する。

【解決手段】 光子を順次発生させ、この順次発生する光子からそれぞれ送信しようとする情報に応じて偏光状態が変化された第1の光子を、またそれぞれ量子力学的に互いに相関する偏光を有する第2と第3の光子を発生させる。送信者は、同時に現れる第1と第2の光子の偏光状態をそれぞれ順次測定してその測定結果を古典通信路を介して受信者に送信し、一方、受信者は、第2の光子と量子力学的に相関して現れる第3の光子の偏光状態を順次測定し、その測定結果と送信者から送信される測定結果から第1の光子の偏光状態の係数を再現し送信者が送信しようとした情報を取り出す。第1の光子のx、y方向の偏光成分の絶対値に含まれる情報並びにその位相差に含まれる情報を取り出すことができ、盗聴から高度に保護された量子通信が可能になる。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 量子状態を送信者から受信者に送信する量子通信方法において、
 光子を順次発生させ、
 前記順次発生する光子からそれぞれ送信しようとする情報に応じて偏光状態が変化された第1の光子を発生させ、
 前記順次発生する光子からそれぞれ量子力学的に互いに相関する偏光を有する第2と第3の光子を発生させ、
 送信者は、同時に現れる第1と第2の光子の偏光状態をそれぞれ順次測定してその測定結果を古典通信路を介して受信者に送信し、
 受信者は、第2の光子と量子力学的に相関して現れる第3の光子の偏光状態を順次測定し、その測定結果と送信者から送信される測定結果から第1の光子の偏光状態の係数を再現し送信者が送信しようとした情報を取り出すことを特徴とする量子通信方法。

【請求項2】 第1の光子のx、y方向の偏光成分の係数の絶対値に含まれる情報を取り出すことを特徴とする請求項1に記載の量子通信方法。

【請求項3】 第1の光子のx、y方向の偏光成分の係数の位相差に含まれる情報を取り出すことを特徴とする請求項1または2に記載の量子通信方法。

【請求項4】 量子状態を送信者から受信者に送信する量子通信装置において、
 光子を順次発生させる手段と、
 前記順次発生する光子からそれぞれ送信しようとする情報に応じて偏光状態が変化された第1の光子を発生させる手段と、
 前記順次発生する光子からそれぞれ量子力学的に互いに相関する偏光を有する第2と第3の光子を発生させる手段とを備え、
 送信者は、同時に現れる第1と第2の光子の偏光状態をそれぞれ順次測定してその測定結果を古典通信路を介して受信者に送信し、
 受信者は、第2の光子と量子力学的に相関して現れる第3の光子の偏光状態を順次測定し、その測定結果と送信者から送信される測定結果から第1の光子の偏光状態の係数を再現し送信者が送信しようとした情報を取り出すことを特徴とする量子通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、量子通信方法及び装置、さらに詳細には、量子力学的状態を送信者から受信者に送信する量子通信方法及び装置に関する。

【0002】

【従来の技術】 現在の情報通信は、通信路を経由しての古典ビット(bits)、即ち0、1を直接送信することにより行なわれており、近年の情報通信網の急激な発達と共に、暗号通信など、通信の機密保持、送受信相手

の確認が大きな課題となっている。

【0003】 一方、近未来の量子情報通信は、2状態系(量子ビット(qubits)、実用的には光の偏光)の任意の重ね合わせ状態に、古典ビットを符号化(encoding)して送信するものである。この状態の送信は、いかなる量子ビットも通信路を経由せず、量子遠隔輸送(quantum teleportation)により可能であるため、情報通信の際の安全(security)の保証が得られる。

【0004】 このような量子情報通信は、例えば、1993年、アメリカのベネット(C. H. Bennett)達により提案されている(29 MARCH 1993, VOLUME 70 NUMBER 13 フィジカル レビュー レターズ(PHYSICAL REVIEW LETTERS 1895-1899ページ)。この方法では、送信者と受信者の間で、あらかじめ量子力学的にもつれた粒子のペア(EPRペア)

が共有されており、送信者は、送りたい情報を符号化した粒子と送信者の持っている粒子(EPRペアの一方)の合成系で、ある物理量の測定を行なう。送信者は、送信者の観測する2粒子系の4つの可能な測定結果の内、1/4の確率で1つの測定結果を得るので、その測定結果を古典通信路で受信者に知らせる。受信者は、送信者から古典通信路を介して送られてくる測定結果に基づき、受信者が保有しているEPRペアのもう一方の粒子を操作することにより送信者が符号化した粒子の状態、即ち量子ビットを再現し、これを復号(decoding)して1ビットの送信を完了させることができる。

【0005】 このテレポーテーション(teleportation)は、量子ビット(粒子[1])の全情報を古典通信路と量子ルートに分け、古典通信路を介して2ビットの情報として伝達するとともに(4つの測定結果は2ビットで表現できる)、EPRペア(粒子[2]、[3])の量子力学的なもつれを量子ルートを介して保有することにより、測定により量子状態が破壊された粒子[1]の量子状態を受信者の保有する粒子[3]において再現することができることを特徴としている。このテレポーテーションでの量子ルートには、量子力学的なもつれによる相関が存在するだけで、古典通信路のような通信路があるわけではないので、通信路を介した盗聴はそもそも有り得ず、また古典通信路を介した情報は盗聴されてもその情報だけでは粒子[1]の量子状態を再現することはできないので、絶対的に盗聴不可能な量子通信が可能になると、いわれている。

【0006】

【発明が解決しようとする課題】 この量子ビットのテレポーテーションという通信技術では、量子力学でEPR問題と呼ばれるものの正しい理解と合理的な観測理論が不可欠であり、重要な役割を果たす。ところがベネツ

ト達の方法は、EPR問題の不明朗な扱いと、量子力学誕生の頃(1926年)のノイマン(von Neumann)の射影仮説と呼ばれる観測理論に基づいており、この仮説を採用しない限り実現が困難である(送信者側で測定により破壊された量子ビットを受信者側で再現する操作が複雑である)。今日では、ノイマンの射影仮説を認めると、物理過程として説明できない現象(否定的測定実験、中性子干渉実験など)が見つかり、又この仮説によるとEPR問題は物理的に説明不可能なパラドックス(EPRパラドックスと呼ばれている)となり、哲学的議論にたよるしかなく、自然法則に従う物理の問題ではなくなる。

【0007】従って、本発明は、このような問題点に鑑みてなされたもので、量子ビットのテレポーテーションの考え方を実現できる量子通信方法及び装置を提供することを課題とする。

【0008】

【課題を解決するための手段】本発明は、この課題を解決するために、量子状態を送信者から受信者に送信する量子通信方法において、光子を順次発生させ、前記順次発生する光子からそれぞれ送信しようとする情報に応じて偏光状態が変化された第1の光子を発生させ、前記順次発生する光子からそれぞれ量子力学的に互いに相関する偏光を有する第2と第3の光子を発生させ、送信者は、同時に現れる第1と第2の光子の偏光状態をそれぞれ順次測定してその測定結果を古典通信路を介して受信者に送信し、受信者は、第2の光子と量子力学的に相関して現れる第3の光子の偏光状態を順次測定し、その測定結果と送信者から送信される測定結果から第1の光子の偏光状態の係数を再現し送信者が送信しようとした情報を取り出す構成を採用した。

【0009】また、本発明では、量子状態を送信者から受信者に送信する量子通信装置において、光子を順次発生させる手段と、前記順次発生する光子からそれぞれ送信しようとする情報に応じて偏光状態が変化された第1の光子を発生させる手段と、前記順次発生する光子からそれぞれ量子力学的に互いに相関する偏光を有する第2と第3の光子を発生させる手段とを備え、送信者は、同時に現れる第1と第2の光子の偏光状態をそれぞれ順次測定してその測定結果を古典通信路を介して受信者に送信し、受信者は、第2の光子と量子力学的に相関して現れる第3の光子の偏光状態を順次測定し、その測定結果と送信者から送信される測定結果から第1の光子の偏光状態の係数を再現し送信者が送信しようとした情報を取り出す構成も採用している。

【0010】

【発明の実施の形態】〔原理の説明〕テレポーテーションによる量子通信を理解するためには、粒子の物理量の測定過程を理解することが不可欠になる。測定過程を物理過程として、現在の量子力学の枠内で合理的に説明

する観測理論は、量子力学の誕生以来、紆余曲折の末、1980年、町田一並木理論として提唱されている。この理論では、測定過程で起こるのは、ノイマンの射影仮説のように分波の消失ではなく量子力学的干渉可能性の消失であり、この過程を記述するには、量子力学で通常考えられているように量子力学的状態を波動関数で記述するのではなく、密度行列(統計作用素、密度作用素とも呼ばれている)で記述しなければならないことが主張されている。

【0011】又この場合、測定される系と測定装置で複合系をなしており、EPR問題は2粒子の複合系とその部分系での測定の問題であり、テレポーテーションは3粒子の複合系とその部分系での測定の問題である。このように測定過程や複合系とその部分系を扱うときは、量子力学的状態は密度行列で記述しなければならない。この考えに沿ってEPR問題を密度行列で記述し、角運動量の保存法則を用いると、どこにもパラドックスは存在せず、EPR問題は正しく合理的に理解できることを町田(1991年)は示した。これに対して、ベネット達の方法では、この保存法則の重要性への認識がなく、測定する物理量も明瞭ではない。

【0012】本発明は、保存法則が成立するよく知られた物理量を観測することによりテレポーテーションの考え方による量子通信を実現しようとするものであり、町田一並木理論に基づき量子力学的状態を密度行列で記述することによりこの量子通信を完全に理解することができるので、以下で説明する実施形態では、量子力学的状態を密度行列で記述することにする。

【0013】古典ビット「0」、「1」は、量子ビット(qubit)では、それぞれ

【0014】

【数1】

$$\begin{aligned} |\phi_0\rangle &= a_0|\uparrow\rangle + b_0|\downarrow\rangle \\ |\phi_1\rangle &= a_1|\uparrow\rangle + b_1|\downarrow\rangle \end{aligned}$$

で表現される。ここで、 $|\phi_i\rangle$ ($i=0, 1$) は、粒子[1]の送信しようとする量子状態で、ディラックのケット表記 $|\rangle$ を用いた粒子[1]の状態ベクトルである。粒子[1]を電子とすると、電子の状態ベクトルは、上向きのスピン \uparrow 状態と下向きのスピン \downarrow 状態の重ね合わせで表現される。 a_i 、 b_i を任意の複素数として、

【0015】

【数2】

$$|a_i|^2 + |b_i|^2 = 1$$

の関係があるので、古典ビット「0」は、スピンの上下成分を測定すれば、状態 $|\uparrow\rangle$ が a_0 の絶対値の2乗の確率で、また状態 $|\downarrow\rangle$ が b_0 の絶対値の2乗の確率で

現れる波動の重ね合わせで表現される量子ビット $|\phi_0\rangle$ に対応し、また古典ビット「1」は、スピンの上下成分を測定すれば、状態 $|\uparrow\rangle$ が a_1 の絶対値の2乗の確率で、また状態 $|\downarrow\rangle$ が b_1 の絶対値の2乗の確率で現れる波動の重ね合わせで表現される量子ビット $|\phi_1\rangle$ に対応する。

【0016】量子力学的にもつれた100%の相関をもつ2個の補助粒子は、EPRペア（EPRは、Einstein-Podolsky-Rosenの頭文字）とも呼ばれており、例えば、スピン1重項（singlet）、即ち全スピンの大きさが0で上下成分もゼロの状態にあるスピン1/2の2電子で実現される。この状態 Ψ のケットは、

【0017】

【数3】

$$|\Psi^{(-)}\rangle_{12} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2)$$

で定式化される。ここで、 $|\uparrow\rangle_1|\downarrow\rangle_2$ は一方の電子[1]がスピン上向き状態に、他方の電子[2]がスピン下向き状態にあり、一方 $|\downarrow\rangle_1|\uparrow\rangle_2$ は一方の電子[1]がスピン下向き状態に、他方の電子[2]がスピン上向き状態にあって、もしスピンの上下成分を測定す

$$\hat{\rho}_{12} \rightarrow \hat{\rho}_{12,\infty} = \frac{1}{2}(|\uparrow\rangle_1\langle\uparrow| \otimes |\downarrow\rangle_2\langle\downarrow| + |\downarrow\rangle_1\langle\downarrow| \otimes |\uparrow\rangle_2\langle\uparrow|)$$

に変換される（ ∞ は、測定後所定の時間が経過したことを示す）。この密度行列の変化は、もつれがほぼ干渉項が消えて全系が混合状態となったことを示している。

また、測定後各粒子の状態は、それぞれ

【0021】

【数6】

$$\begin{aligned}\hat{\rho}_1 &\rightarrow \hat{\rho}_{1,\infty} = \text{Tr}^{(2)}(\hat{\rho}_{12,\infty}) = \hat{\rho}_1 \\ \hat{\rho}_2 &\rightarrow \hat{\rho}_{2,\infty} = \text{Tr}^{(1)}(\hat{\rho}_{12,\infty}) = \hat{\rho}_2\end{aligned}$$

となる。但し、

【0022】

【数7】

$$\text{Tr}^{(*)}$$

は部分トレース（行列の対角要素の和を部分的にとる）を示す。

【0023】数6の第2式は、他方の粒子[2]の量子力学的状態は、一方の粒子[1]の測定によって何の変化も受けていないことを示しているので、量子状態を数3のように記述した場合に発生するEPRパラドックスを回避することができる。

【0024】ここで、上述した量子力学的にもつれた状態を含む2個の粒子（EPRペアの拡張）を補助粒子として使い、送信しようとする古典ビットに応じた量子ビットをテレポーテーションする量子通信の具体的な

れば、それぞれ1/2の確率で $|\uparrow\rangle_1|\downarrow\rangle_2$ あるいは $|\downarrow\rangle_1|\uparrow\rangle_2$ が観測されることを示している。これらの補助粒子は、量子力学的にもつれた状態にあり、100%相関しているので、これらがたとえ巨視的距離離れていたとしても、一方の粒子のスピン状態が上向きと観測されれば（50%の確率）、他方の粒子のスピン状態の観測結果を確実に（100%）下向きであると予言できることを示している。

【0018】フォン・ノイマンの射影仮説に従いEPRペアを数3のように記述すると、いわゆるEPRパラドックスが発生する。測定により純粋状態は、混合状態へと変化するので、EPRペアの量子状態は、統計作用素（密度行列） ρ を用いて、

【0019】

【数4】

$$\hat{\rho}_{12} = |\Psi^{(-)}\rangle_{12}\langle\Psi^{(-)}|$$

のように記述しなければならない。この密度行列の記述で、一方の粒子のスピンの上下成分の測定後の全体の系の状態は

【0020】

【数5】

方法を説明する。

【0025】図1に示したように、送信者10は、送信しようとする古典情報に応じて符号化された量子ビット $|\phi_i\rangle_i$ （古典ビット「0」、「1」に応じて $i=0, 1$ 、 $|\phi_0\rangle_i$ と $|\phi_1\rangle_i$ は非直交状態にある）と、その直交状態 $|\psi_i\rangle_i$ である粒子[1]のブロック11を用意する。

【0026】また、送、受信者は、量子力学的にもつれた状態を含む2個の補助粒子[2]、[3]を準備し、一方の粒子[2]を送信者10が、また他方の粒子[3]を受信者12が保有する。そして、送、受信者は粒子[2]と[3]の合成系14で角運動量の大きさ1、そのz-成分が0、1、-1の3つの状態 $|1, 0\rangle_{12}$ 、 $|1, 1\rangle_{12}$ 、 $|1, -1\rangle_{12}$ を共有する。また、送信者10は、これらの3つの状態と粒子[1]の積状態 $|\phi_i\rangle_i|1, 0\rangle_{12}$ 、 $|\psi_i\rangle_i|1, 1\rangle_{12}$ 、 $|\psi_i\rangle_i|1, -1\rangle_{12}$ を作り、これを2:1:1の強度比で混ぜた混合状態16を作る。この全系の状態を密度行列を用いて記述すると、 $|1, 0\rangle = |\Psi^{(+)}\rangle$ 、 $|1, 1\rangle = |\uparrow\rangle$ 、 $|1, -1\rangle = |\downarrow\rangle$ と書いて、

【0027】

【数8】

$$\hat{\rho}_{1,23} = \frac{1}{4} \{ |\psi\rangle_1 \langle\psi| \otimes |1\rangle_{23} \langle 1| + |\psi\rangle_1 \langle\psi| \otimes |-1\rangle_{23} \langle -1| + 2|\phi\rangle_1 \langle\phi| \otimes |\Psi^{(*)}\rangle_{23} \langle\Psi^{(*)}| \}$$

のようになる。但し

【0028】

【数9】

$$\begin{aligned} |\phi\rangle &= a|\uparrow\rangle + b|\downarrow\rangle \\ |\psi\rangle &= -b^*|\uparrow\rangle + a^*|\downarrow\rangle \\ |\Psi^{(*)}\rangle &= \frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle + |\downarrow\rangle|\uparrow\rangle) \end{aligned}$$

である。部分トレースをとることにより、ブロック1

1、14に対応する

【0029】

【数10】

$$\hat{\rho}_1 = Tr^{(23)}(\hat{\rho}_{1,23}) = \frac{1}{2} \{ |\psi\rangle_1 \langle\psi| + |\phi\rangle_1 \langle\phi| \}$$

$$\hat{\rho}_{23} = Tr^{(1)}(\hat{\rho}_{1,23}) = \frac{1}{4} \{ |1\rangle_{23} \langle 1| + |-1\rangle_{23} \langle -1| + 2|\Psi^{(*)}\rangle_{23} \langle\Psi^{(*)}| \}$$

が得られ、上記の(1, 23)系を(12, 3)系に組

【0030】

み直すことにより、ブロック18と20に対応する

【数11】

$$\hat{\rho}_3 = Tr^{(12)}(\hat{\rho}_{12,3}) = \frac{1}{2} \{ |\psi\rangle_3 \langle\psi| + |\phi\rangle_3 \langle\phi| \}$$

$$\hat{\rho}_{12} = Tr^{(3)}(\hat{\rho}_{12,3}) = \frac{1}{4} \{ |1\rangle_{12} \langle 1| + |-1\rangle_{12} \langle -1| + |\Psi^{(*)}\rangle_{12} \langle\Psi^{(*)}| + |\Psi^{(-)}\rangle_{12} \langle\Psi^{(-)}| \}$$

が得られる。

列は、

【0031】次に、送信者10は自分の保有する粒子

【0032】

【1】と【2】からなる(1, 2)系18で角運動量の

【数12】

z-成分の測定を行なう。この測定により全系の密度行

$$\begin{aligned} \hat{\rho}_{12,3} &\rightarrow \hat{\rho}_{12,3,\infty} \\ &= \frac{1}{4} \{ |1\rangle_{12} \langle 1| + |-1\rangle_{12} \langle -1| \otimes |b|^2 |\uparrow\rangle_3 \langle\uparrow| + |a|^2 |\downarrow\rangle_3 \langle\downarrow| \} \\ &\quad + \frac{1}{2} |\Psi^{(*)}\rangle_{12} \langle\Psi^{(*)}| \otimes \{ 2|a|^2 |\uparrow\rangle_3 \langle\uparrow| + 2|b|^2 |\downarrow\rangle_3 \langle\downarrow| + ab^* |\uparrow\rangle_3 \langle\downarrow| + a^*b |\downarrow\rangle_3 \langle\uparrow| \} \\ &\quad + \frac{1}{2} |\Psi^{(-)}\rangle_{12} \langle\Psi^{(-)}| \otimes \{ 2|a|^2 |\uparrow\rangle_3 \langle\uparrow| + 2|b|^2 |\downarrow\rangle_3 \langle\downarrow| - ab^* |\uparrow\rangle_3 \langle\downarrow| - a^*b |\downarrow\rangle_3 \langle\uparrow| \} \end{aligned}$$

のように変換され、最終的に

【0033】

【数13】

$$\hat{\rho}_{3,\infty} = Tr^{(12)}(\hat{\rho}_{12,3,\infty}) = \hat{\rho}_3$$

$$\hat{\rho}_{12,\infty} = Tr^{(3)}(\hat{\rho}_{12,3,\infty}) = \hat{\rho}_{12}$$

を得る。

【0034】送信者10は、(1, 2)系の測定により0又は±1の測定結果を得るので、その測定結果(又は、測定が完了したこと)を古典通信路で受信者12に知らせる。この情報を受け取った受信者12は自分の持つ粒子【3】の状態20に、それぞれ $|\phi_1\rangle$ 、又は $|\psi_1\rangle$ が現れたことを角運動量の保存法則から知り、受信者は粒子【3】の測定による復号化で $|\phi_0\rangle$ 、又は $|\psi_0\rangle$ が送られたことを知ることができる。

【0035】古典ビット0、1の符号化、復号化の方向及びz軸の方向は、あらかじめ送受信者で決めておいてもよいし、復号化の際の測定結果の確率の差から読み出すこともできる。この方法は、ベネット達のものとは違い、送信者側で測定により破壊された量子ビットを受信者側で再現する操作は不要である。

【0036】[光子を用いた第1の実施形態] 上述した原理は、スピン1/2の粒子(電子、中性子など)で可能であるが、実用化に適した光子を粒子とする例に基づきテレポーテーションの具体例を説明する。光の偏光をスピンの代わりに用いる場合は、

【0037】

【数14】

9

$$\begin{aligned} |\leftrightarrow\rangle &= x \\ |\updownarrow\rangle &= y \end{aligned}$$

(x は水平偏光状態、 y は垂直偏光状態)とし、スピン1/2の粒子のスピン状態 $|\uparrow\rangle$ と $|\downarrow\rangle$ を、例えば $|\uparrow\rangle=x$ 、 $|\downarrow\rangle=y$ あるいはその逆に読み替えることで、スピン1/2の粒子について述べたことが、原理的には光子について、全てあてはまる。しかし、3個の光子を用いる場合、光子の偏光状態の測定は1個1個の光子についてしかできず、図1のブロック16である3光子の数8に対応する状態及び図1のブロック18、20である数11を導く3光子の状態の直接の作成は困難などの実際上の制約があるため、光子3個で量子通信を実現するには特別の工夫が必要である。

【0038】図2には、この工夫のなされた粒子を光子とした場合のテレポーテーションの考え方を示した実施形態が図示されている。

【0039】図2は、基本的に重要な部分のみを一つの例で分かり易く示したものであり、同図に示したように、送信者10はブロック21を、受信者12はブロック50を用意する。ブロック21の中で符号22で示すものは、最初の光源としてのレーザーパルス発振器で、ナノ秒程度の間隔で角振動数 ω のパルスを次々と発生する。各レーザーパルスは2次高調波発生結晶(例えば、 KNbO_3 などの結晶、以下SHGという)23に入射される。ここでは、説明の便宜上、パルスレーザーを用いたが、連続波レーザーを用いることも出来る。

【0040】SHG23から、角振動数 ω で素通りした光子と角振動数が 2ω に変わった光子の2光子が得られ、角振動数 ω の光子は光子[1]のブロック30へ、角振動数 2ω の光子は、例えば KNbO_3 などのタイプIの非線形結晶から構成されるパラメトリック変換器(パラメトリック・ダウン・コンバーター、以下PDCという)24へ導かれる。このPDC24で、角振動数 ω の2光子に変換され、一方の光子は、送信者側の光子[2]のブロック40へ、もう一方の光子は光ファイバー25を経由して受信者側の光子[3]のブロック50へ送られる。PDC24から出た2光子はタイプIの結晶の場合、その偏光状態が互いに x (水平偏光)同士、又は互いに y (垂直偏光)同士と決まった所定の偏光状態で放出される。

【0041】以下、光子[1]のブロック30、光子[2]のブロック40、光子[3]のブロック50の順に説明する。

【0042】SHG23からブロック30に導かれた光子[1]はハーフミラー31で2つの光路に分割され、ハーフミラー31を通過した光子は偏光回転子(水晶、ファラデー回転子という)32を通り、偏光方向が θ 回転されて $|\phi\rangle$ 状態が形成される。垂直偏光(y)を通過させ、水平偏光(x)を反射する偏光ビームスプリ

10

ッター(以下PBSという)33で、偏光方向が θ 回転された光子は、 θ に対応する係数 a 、 b を持つ $a x_1$ と $b y_1$ に分割され、 $b y_1$ はそのまま光電子増倍管62へ、また $a x_1$ はミラー34で反射された後光電子増倍管61へ導かれる。

【0043】一方、ハーフミラー31で反射された光はミラー35で反射され偏光回転子(ファラデー回転子)36で偏光方向が $\pi/2$ 回転され、 $|\psi\rangle$ 状態が形成される。この $\pi/2$ 偏光が回転された光子は、その後PBS37で、 $(\theta+\pi/2)$ に対応する係数 a' 、 $-b'$ をもつ $a' y_1$ と $-b' x_1$ に分割され、 $a' y_1$ はそのまま光電子増倍管64へ、 $-b' x_1$ はミラー38で反射され光電子増倍管63へと導かれる。

【0044】この光子[1]のブロック30は、図1の光子[1]のブロック11に対応し、量子ビット $|\phi\rangle$ の光子と、その直交状態 $|\psi\rangle$ の光子が形成されたことになる。その場合、古典ビット「0」、「1」は偏光回転子32、36で偏光方向 θ をそれに対応して設定することにより量子ビットに変換することができる。

【0045】PDC24からブロック40に導かれた光子[2]は、偏光状態はそのまま、ハーフミラー41で2つの光路に分割され、ハーフミラー41を通過した方は、PBS43で偏光 x_2 と y_2 の光子に分割され、偏光 y_2 の光子はそのまま光電子増倍管72へ、偏光 x_2 の光子はミラー42で反射された後、光電子増倍管71へ導かれる。一方ハーフミラー41で反射された方はミラー44で反射された後PBS45で偏光 x_2 と y_2 の光子に分割され、偏光 y_2 の光子はそのまま光電子増倍管73へ、偏光 x_2 の光子はミラー46で反射された後光電子増倍管74へと導かれる。

【0046】PDC24から、光ファイバー25を経由して受信者側のブロック50へ送られた光子[3]はハーフミラー51で2つの光路に分割され、ハーフミラー51を通過した方はPBS52で偏光 x_3 、 y_3 の光子に分割され偏光 y_3 の光子はそのまま光電子増倍管82へ、偏光 x_3 の光子はミラー53で反射された後光電子増倍管81へと導かれる。ハーフミラー51で反射された方は $\lambda/2$ の半波長板54で x 偏光と y 偏光が入れ換えられた後、ミラー55で反射されPBS56で偏光 x_3 と y_3 の光子に分割され、偏光 y_3 の光子はそのまま光電子増倍管83へ、偏光 x_3 の光子はミラー57で反射された後光電子増倍管84へと導かれる。

【0047】この装置では、レーザーパルス発生器22の各パルスごとにブロック30の光電子増倍管61~64のどれか、ブロック40の光電子増倍管71~74のどれか、ブロック50の光電子増倍管81~84のどれかに、それぞれ光子が1個づつ現れるので、光子[1]と光子[2]で作る部分系で送信者が行う測定は、図3に図示したように、2つのペア端子で、それぞれ偏光をカウンタ111~118を用いて同時計数を行うこと

により行なわれる。

【0048】カウンタ111～114は、光電子増倍管63と71、61と74、62と73、64と72の各ベアからの光子が同時に現れる順序と回数を計数し、係数 a 、 b に対応した計数確率 b 、 a 、 b 、 a の絶対値の2乗がそれぞれカウンタの出力端子91～94に得られる。

【0049】同様に、カウンタ115～118は、光電子増倍管61と73、63と72、64と71、62と74の各ベアからの光子が同時に現れる順序と回数を計数し、係数 a 、 b に対応した計数確率 a 、 b 、 a 、 b の絶対値の2乗がそれぞれカウンタの出力端子95～98に得られる。

【0050】この測定結果を与えるパルスごとの同時計数、すなわち、カウンタの出力端子91～98のどの端子に同時計数が得られたかと、その計数順序を受信者に古典通信する。受信者側では、光電子増倍管81～84に附属のどの端子に光子が現れたかを測定し、その順序を記録しておく、図4に示したように、古典通信の結果に応じて、それぞれ測定端子が101～108のように決まるので、それぞれの決まった測定端子に古典通信で送られた送信者の同時計数順序に、91と101、92と102、…、98と108に同時計数の得られた記録と照合し、3光子の同時計数の得られた結果のみを集め、その回数を計数すると、結果が対応する確率で101～108のように得られる。端子101～104では、確率 b の絶対値の2乗で x_i が、また確率 a の絶対値の2乗で y_i が得られるので、端子101～104より $|\psi\rangle_i$ が送られたことがわかる。また端子105～108では、確率 a の絶対値の2乗で x_i が、また確率 b の絶対値の2乗で y_i が得られるので、端子105～108より $|\phi\rangle_i$ が送られたことがわかる。例えば、送信者10は「0」の1ビットを送信しようとする。そこで、図2のレーザーパルス光源22からナノ秒程度の間隔でパルスを順次発生させ、偏光回転子32と36で「0」に対応して θ を任意に決める。これにより偏光回転子32、36により「0」に対応した係数 a の水平偏光 x_i と係数 b の垂直偏光 y_i の重ね合わせからなる量子状態 $|\phi\rangle_i$ とその直交状態の $|\psi\rangle_i$ が得られる(光子[1])。PDC24により所定の偏光 x/y を有する光子[2]、光子[3]を作成し、光子[3]を光ファイバー25を介して受信者12に送る。

【0051】送信者10は、光源22からのレーザーパルスを100パルス(10のマイナス7乗秒)～1000パルス(10のマイナス6乗秒)についてカウンタ111～118を用いて同時計数する。量子力学に従って起こる現象は確率的であるので、その測定結果が「0」に応じた係数 a 、 b に対応する上記のような計数確率として得られる。そこで、送信者10はカウンタの出力端子91～98のどの端子に同時計数が得られたかと、

その順序を古典通信路を用いて受信者12に送信する。

【0052】光子[3]を測定する受信者12の測定端子 a_i 、 a_j 、 b_i 、 b_j は、送信者10の光子[2]の測定端子 A_i 、 A_j 、 B_i 、 B_j とそれぞれ対応(相関)しており、各測定端子101～108には、それぞれ水平偏光ないし垂直偏光が現れる。従って、受信者12は、光電子増倍管81～84に附属のどの端子に光子が現れたかを測定し、その順序を記録しておき、パルスごとの送信者側での同時計数結果の古典通信に応じて定まった測定端子に光子が現れた記録、つまり91と101、92と102、…、98と108に同時計数の得られた記録と照合し、その結果を集めると、水平偏光(x_i)の現れる測定端子101、103と垂直偏光(y_i)に現れる測定端子102、104とから、受信者12は、係数 $-b'$ の水平偏光 x_i と係数 a' の垂直偏光 y_i を受信することができ、 $|\psi\rangle_i$ が送信されたことを知ることができる。このとき、同様に測定端子105～108を介して $|\phi\rangle_i$ が送信されたことを知ることができる。

【0053】一方、送信者10が「1」の1ビットを送信しようとする場合には、それに応じて「0」の送信時と異なる量だけ θ (その差が0、 π 以外の任意の角度)を変化させる。それに応じて係数 a 、 b が変化し、計数確率も変化して「1」に対応する $|\psi\rangle_i$ 、 $|\phi\rangle_i$ の係数を受信することができ、 $|\psi\rangle_i$ 、 $|\phi\rangle_i$ が送信されたことを知ることができる。

【0054】図7は、上述したシーケンスを理解するために、送信者による光子[1]と[2]の同時計数と、受信者の測定結果と古典通信間の相関を示すタイミング図である。図示を簡略にするために、図2の光子[1]～[3]の各光学チャンネル対の半分のみが図示されている。

【0055】レーザーパルス発振器22から一つの光子が発生すると、それぞれ光子[1]、[2]、[3]がブロック30、40及び50に生成される。このように生成された光子[1]は係数 a と b に関係した確率で光電子増倍管61～64のいずれかに、光子[2]は4分の1の確率で光電子増倍管71～74のいずれかに、また光子[3]も4分の1の確率で光電子増倍管81～84のいずれかに現れる。図7には、レーザーパルス発振器22から順次光子が発生したとき、光電子増倍管61と62、73と74、83と84にランダムに順次現れる光子[1]～[3]がそれぞれ図示されている。

【0056】送信者10は、図7に示したように、端子95、92、93、…において光子[1]と[2]が同時に現れ同時計数が得られたことを測定する。一方、受信者は光子[3]の出現を記録し、送信者は同時計数の結果を古典通信路を介して受信者に送信する。受信者は受信者の記録と古典通信路を介して送信されてきたメッセージとの相関を取り、図7でそれぞれ(*)を付した光子[3]と量子力学的に相関する光子[2]が送信者側で光子[1]と一致計測されていることを知り、(*)

を付した光子[3]が選択すべき光子であることを知る。これは、この時点で3つの光子[1]、[2]及び[3]が同時に出現したことを計測していることを意味している。これら3つの光子が一致して現れるところが図7で垂直線で図示されており、測定結果102、103、108、102、105、...、103、108及び105として示されている。受信者12は、古典ビット「0」が送信された場合には、測定結果102と103から $|\psi_0\rangle$ の係数を、また測定結果105と108から $|\psi_1\rangle$ の係数を取り出し（古典ビット「1」が送信された場合には、 $|\psi_1\rangle$ と $|\psi_0\rangle$ ）、 $|\psi_0\rangle$ と $|\psi_1\rangle$ （ $|\psi_1\rangle$ と $|\psi_0\rangle$ ）が送信されたことを知る。

【0057】光子[1]の量子状態に書き込まれた情報を受信者で再現するには、古典通信路を介して送信されてくるパルスごとの同時計数結果と、光ファイバー25から送られてくる光子[3]の偏光状態（光子[2]の偏光状態に相関する）を知る必要があるので、古典通信路を介して送られるパルスごとの同時計数結果だけ盗聴しても、あるいは光ファイバーを通過する光子[3]の偏光状態だけを測定しても、光子[1]の量子状態に書き込まれた情報を再現することはできない。

【0058】通信路には、いかなる情報も持たぬ偏光した光子が通っているだけであるから、通信路25における盗聴は全く不可能である。すなわち、量子ルート（通信路25）は、単なる偏光光子が通過するだけであり、古典通信路には受信者の測定端子を決める情報が流れるだけなので、100～1000パルスの情報を集めないと、送信者から送られた情報が「0」か「1」かがわからない。したがって、通信路25を介しての盗聴があり、パルスの数が1/2になると、受信者も盗聴者も送信者からの情報を再生することが不可能になる。この意味で通信の破壊は可能であるが、送信者と受信者の間で「0」か「1」のどちらかのa、bを一つ決めておくと、受信者では、送信者の情報を再現できるが、盗聴者にはどのような情報が送られてきたのか不明であるようにすることができる。

【0059】光子を用いたテレポーテーションでは、測定並びに古典通信が【原理の説明】で図1を用いて説明したものよりも複雑になるが、これは【原理の説明】の最後に述べた光子を用いる場合の特別な事情による。なお、受信者の測定は送信者からの古典通信に応じて自動化して記録しておけば、後で読み出すことができる。

【0060】ここで、端子91～94での測定結果は、スピン測定の場合の±1に、端子95～98の測定結果は0に対応しているので光電子増倍管61～64、71～74の測定端子にエレクトロニクスでAND、ORの回路を組むことにより、送信者での測定及び送信者からの古典通信を簡単化することができる。受信者での端子101～108の測定も同様に簡単化できるが、端子1

01～108の測定は、あらかじめ送受信者間で偏光回転子32と36の θ を決めておくことにより、 $|\psi_0\rangle$ と $|\psi_1\rangle$ の測定におき換えることにより簡単化することもできる。

【0061】図2において、光子[1]のブロック30が数10の第1式に、ブロック40とブロック50が数10の第2式に対応する。又、端子91～98の測定後のブロック21が数11の第2式に、その時のブロック50が数11の第1式に対応する。同じく端子91～98の測定後のブロック21と50の全体は数12に対応する。しかし、【原理の説明】の最後に述べた事情により、これらの対応は数10、数11あるいは数12と全く同じという意味ではなく、量子通信として【原理の説明】で述べたことと同じ結果を与えるという意味での対応である。

【0062】図2では、ブロック30、40、50の間で【原理の説明】で述べた部分的に必要な光の強度調整（フィルター又はダミーミラーを用いる）と光電子増倍管61～64、71～74及び81～84に光が測定器の応答時間内に同時到着するための光路長調整は簡単に行うことができるが、図が不必要に複雑にならないように省略してある。又、PDC結晶の温度調整なども当然のことなので省略してある。その他、通信精度向上、測定精度向上のための偏光子なども省略されているが、いずれも必要に応じて適宜設けられるものである。

【0063】さらに、PDC24のタイプIをタイプIIにするとか、偏光ビームスプリッターの代わりに入/2の半波長板を用いるとか、 θ の偏光回転子を透過度と反射度が50:50でないハーフミラーにおき換えるなど色々の光学素子の入れ換えが可能であり、その時、図も変わってくるが、図2では、基本的に重要な部分のみが一例として示されている。

【0064】また、図2において、主要な光学素子とその配置を変えずに、いくつかの光学素子の入れ替えや、追加等が可能である。例えば、その一つはPDCをタイプIからタイプIIに変更するものである。この場合、上述した通信方法がそのまま当てはまる。

【0065】【光子を用いた第2の実施形態】第1の実施形態では、同時計数確率の重複が多く、aとbの絶対値に書き込まれた「0」か「1」しか送受信できないが、図5に示す第2の実施形態では、aとbの位相差に書き込まれた情報も送受信可能になる。

【0066】図5において、図2と同様な部分には、同じ参照符号を付し、その詳細な説明は省略する。図2に示す実施形態と異なるところは、図2のブロック40中のミラー44とPBS45の間、及びブロック50の半波長板54とミラー55の間に、偏光面内での偏光方向を45°回転するファラデー回転子と呼ばれる光学素子47、58を挿入しているところである。

【0067】このような構成において、光電子増倍管6

3、64の測定端子 ϕ_1 、 ϕ 、並びに光電子増倍管71、72の測定端子 A_1 、 A で、図3に示したような同時計数を行ない、その結果を古典通信を介して受信者に送信する。この古典通信に基づく光電子増倍管81、82の測定端子 a_1 、 a の決定とその測定端子での測定は、図2に示す実施形態と同じであり、これにより a 、 b の絶対値に書き込まれた情報を読み出すことができる。

【0068】一方、光電子増倍管61、62の測定端子 ϕ_1 、 ϕ 、並びに光電子増倍管73、74の測定端子 B_1 、 B での同時計数並びにその古典通信に基づく光電子増倍管83、84の測定端子 b_1 、 b の決定とその測定端子での測定は、ファラデー回転子47、58が設けられていることにより以下ようになる。

【0069】それぞれ光電子増倍管61、74、84の測定端子 ϕ_1 、 B_1 、 b_1 では $\pi/4$ 方向(+方向とする)、また、光電子増倍管62、73、83の測定端子 ϕ_1 、 B_1 、 b_1 では $3\pi/4$ 方向(-方向とする)の偏光測定となり、光子[1]、[2]での同時計数92、93、95、98はそのままだが、光子[3]の測定結果102、103、105、108は光電子増倍管83と84の測定端子 b_1 、 b が入れ替わることによって x と y の偏光が混じり、測定結果が、図6に示したように、111~114と変わる。この変更により同時計数確率が $|a+b|$ の2乗、 $|a-b|$ の2乗に変化し、 a と b の位相差に書き込まれた情報を読み出すことが可能になる。

【0070】このように第2の実施形態では、第1の実施形態に比較して、同時計数確率の重複を半分にできるとともに、 a と b に書き込まれた全ての情報(絶対値に書き込まれた情報並びに位相差に書き込まれた情報)を読み出すことができる。

【0071】[光子を用いた第3の実施形態]第1と第2の実施形態で使用される光電子増倍管61~64、71~74、81~84は光子1個を検出するもので、現在では高価なアバランシェ・フォト・ダイオード(APD)がそれに使用されている。この高価な素子の数を半分に減らし、かつ a と b に書き込まれた全ての情報を読み出すようにすることができる。そのためには、光電子増倍管63、64、71、72の測定端子 ϕ_1 、 ϕ 、 A_1 、 A での同時計数は行なわないことにし、これらの端子にきた光子は逃がすことにする。従って受信者側の光電子増倍管81、82の測定端子 a_1 、 a での測定も行なわないことにする。

【0072】一方、光電子増倍管61、62、73、74の測定端子 ϕ_1 、 ϕ 、 B_1 、 B での同時計数とその結果の古典通信に基づく光電子増倍管83、84の測定端子 b_1 、 b の決定とその測定端子での測定は第1の実施形態と同様に行ない、これから a と b の絶対値に書き込

まれた情報を読み出す。

【0073】その後、第2の実施形態で述べた測定を光電子増倍管61、62、73、74、83、84の測定端子 ϕ_1 、 ϕ 、 B_1 、 B 、 b_1 、 b について行ない、これにより a と b の位相差に書き込まれた情報を読み出すことにする。

【0074】これにより、光電子増倍管としてAPDを用いても、その数を6個に減らすことができ、かつ a と b に書き込まれた全ての情報を読み出すことができる。つまり、ベネット達とは異なるが、この方法では通信の補助に、粒子[2]と[3]の純粋状態を用いるという点でベネット形の通信方法も可能となる、尚、この量子通信では、「0」と「1」の2値通信のみでなく、計数確率の差を読み出せる限りにおいて多値通信も可能であり、暗号表の作成も可能である。

【0075】

【発明の効果】以上説明したように、本発明では、送信者は、同時に現れる第1と第2の光子の偏光状態をそれぞれ順次測定してその測定結果を古典通信路を介して受信者に送信し、一方、受信者は、第2の光子と量子力学的に相関して現れる第3の光子の偏光状態を順次測定し、その測定結果と送信者から送信される測定結果から第1の光子の偏光状態の係数を再現し送信者が送信しようとした情報を取り出すようにしているので、盗聴から高度に保護された量子暗号通信が可能になる。

【図面の簡単な説明】

【図1】量子通信の原理を説明する説明図である。

【図2】粒子を光子とした場合の量子通信装置の構成を示す構成図である。

【図3】光子の偏光成分の同時計数を測定する状態を示した構成図である。

【図4】送信者の同時計数の測定結果を受信者に古典通信する状態を示した説明図である。

【図5】粒子を光子とした場合の量子通信装置の他の構成を示す構成図である。

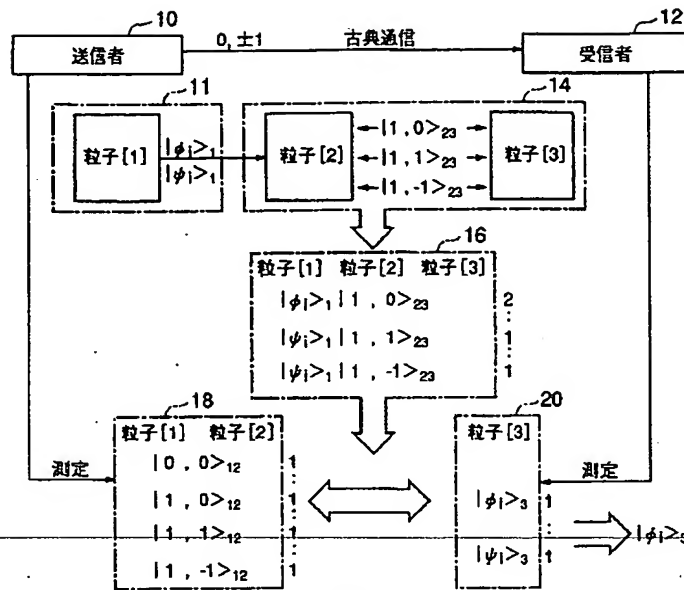
【図6】偏光方向を 45° 回転したときの、送信者の同時計数の測定結果を受信者に古典通信する状態を示した説明図である。

【図7】送信者による光子の同時計数と、受信者の測定結果と古典通信間の相関を示すタイミングチャート図である。

【符号の説明】

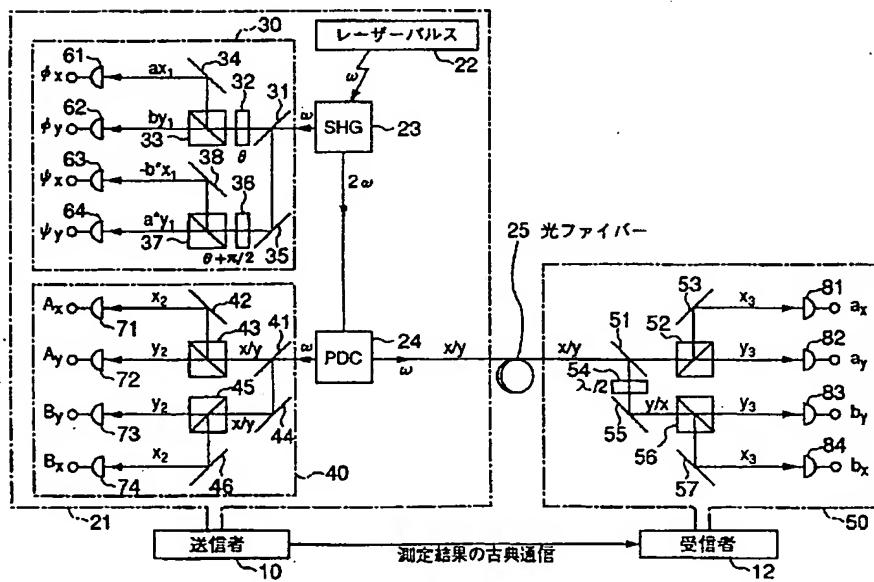
- 10 送信者
- 12 受信者
- 22 レーザーパルス光源
- 23 2次高調波発生結晶
- 24 パラメトリック変換器
- 25 光ファイバー

【図 1】



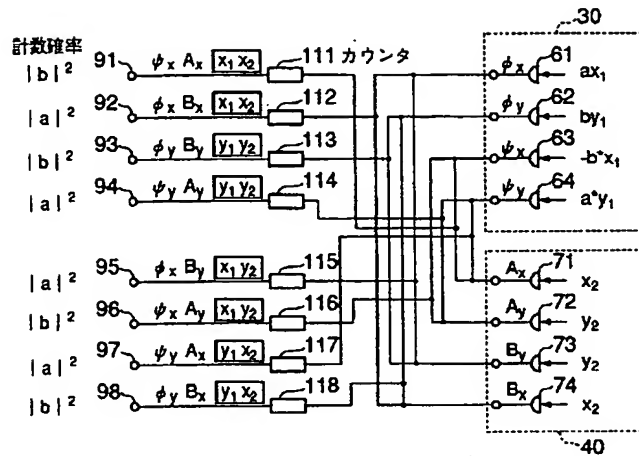
(図 1)

【図 2】



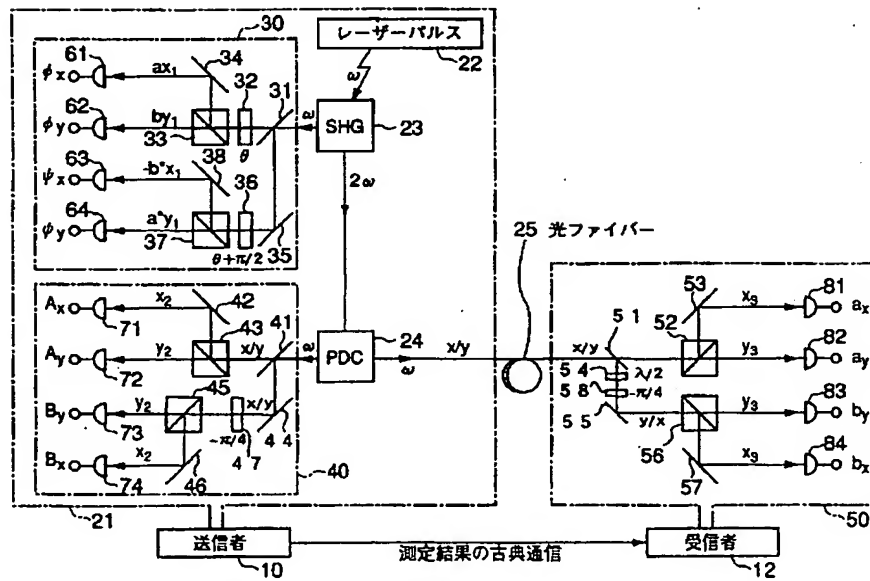
(図 2)

【図 3】



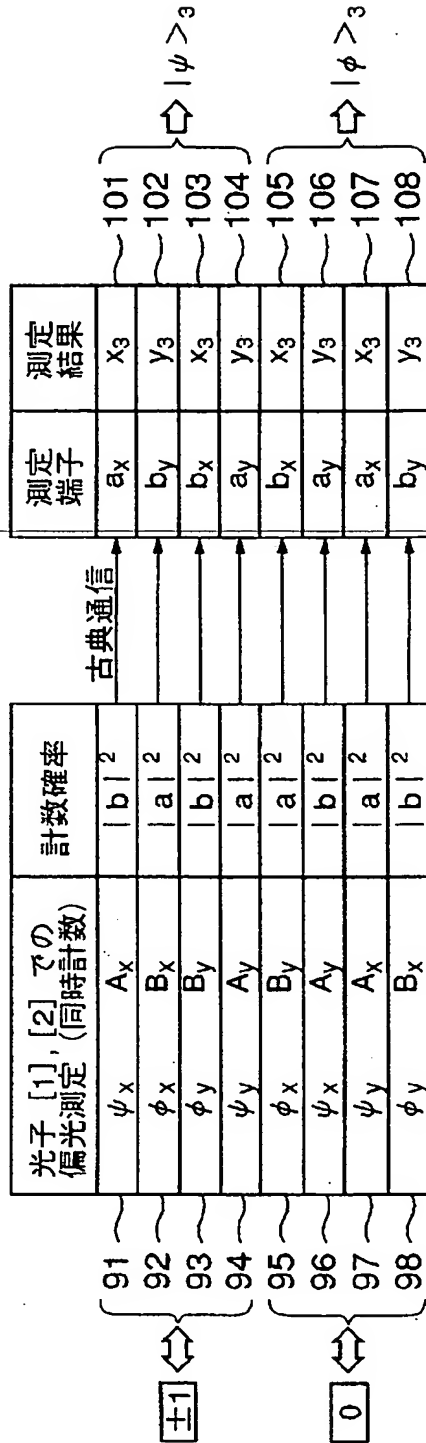
(図 3)

【図 5】



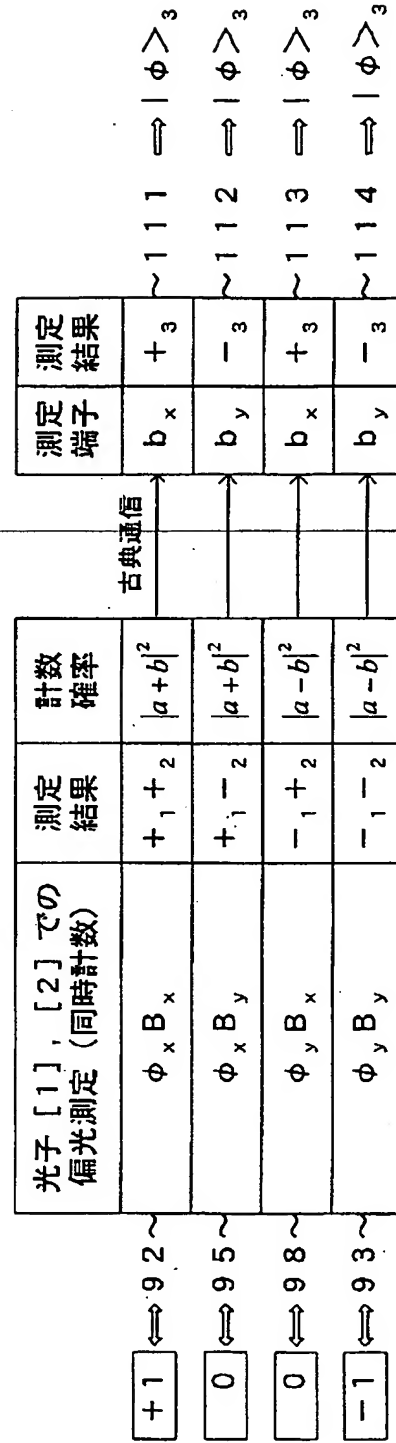
(図 5)

〔図 4〕



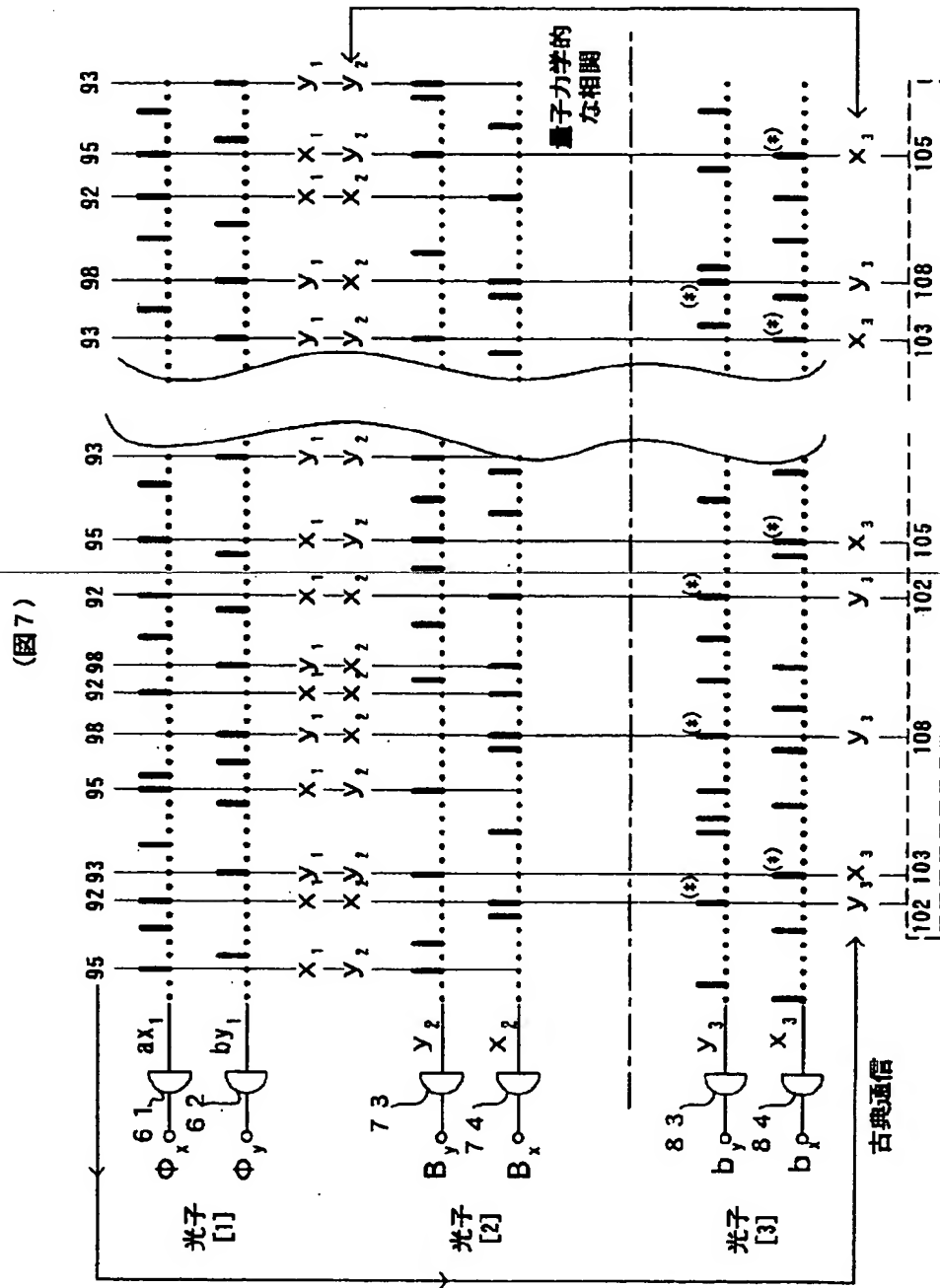
(図 4)

〔図 6〕



(図 6)

【图7】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.